

**NASA  
Technical  
Paper  
1932**

November 1981

NASA-TP-1932 19820003911

# Space Shuttle Main Engine Controller

Russell M. Mattox  
and J. B. White

1981-10-01

1981-10-01

1981-10-01

**NASA**



**NASA  
Technical  
Paper  
1932**

1981

# Space Shuttle Main Engine Controller

Russell M. Mattox  
and J. B. White  
*George C. Marshall Space Flight Center  
Marshall Space Flight Center, Alabama*

**NASA**

National Aeronautics  
and Space Administration

Scientific and Technical  
Information Branch

## ACKNOWLEDGMENTS

The authors would like to express their appreciation to Mr. John Gattis, Mr. Walt Mitchell, and Mr. Claude Boykin who submitted useful comments and suggestions leading to the completion of this document.

# TABLE OF CONTENTS

|  | Page |
|--|------|
| INTRODUCTION .....                             | 1    |
| CONTROLLER ARCHITECTURE AND ORGANIZATION ..... | 2    |
| Redundancy Management .....                    | 4    |
| Digital Computer Unit .....                    | 6    |
| Memory .....                                   | 9    |
| Computer Interface Electronics .....           | 11   |
| Input Electronics .....                        | 15   |
| Output Electronics .....                       | 17   |
| Power Supply Electronics .....                 | 20   |
| PACKAGING .....                                | 22   |
| TESTING .....                                  | 24   |
| Controller Qualification Testing .....         | 25   |
| Acceptance Testing .....                       | 27   |
| Engine/Controller Testing .....                | 29   |
| Laboratory System Testing .....                | 29   |
| OPERATIONAL FUNCTIONS AND TIMELINES .....      | 29   |
| OPERATIONAL EXPERIENCE .....                   | 31   |
| CONCLUSIONS .....                              | 32   |
| BIBLIOGRAPHY .....                             | 33   |

## LIST OF ILLUSTRATIONS

| Figure | Title  | Page |
|--------|--|------|
| 1.     | Controller interfaces . . . . .                | 3    |
| 2.     | Simplified redundancy diagram. . . . .         | 4    |
| 3.     | DCU system configuration . . . . .             | 6    |
| 4.     | Power supply conditioner . . . . .             | 8    |
| 5.     | Memory half-stack module . . . . .             | 9    |
| 6.     | Memory board assembly . . . . .                | 10   |
| 7.     | Tunnel structure/memory plane detail . . . . . | 10   |
| 8.     | Computer interface electronics . . . . .       | 11   |
| 9.     | Input electronics. . . . .                     | 15   |
| 10.    | Output electronics. . . . .                    | 18   |
| 11.    | Power supply. . . . .                          | 21   |
| 12.    | SSME controller . . . . .                      | 23   |
| 13.    | PC board retention design . . . . .            | 24   |
| 14.    | System test configuration . . . . .            | 30   |
| 15.    | Major cycle timing. . . . .                    | 31   |

## SYMBOLS AND ABBREVIATIONS

|       |                                      |
|-------|--------------------------------------|
| SSME  | Space Shuttle Main Engine            |
| DCU   | Digital Computer Unit                |
| NDRO  | Non-Destructive Read Out             |
| PSC   | Power Supply Conditioner             |
| GSE   | Ground Support Equipment             |
| DMA   | Direct Memory Access                 |
| DIO   | Direct Input/Output                  |
| CPU   | Central Processor Unit               |
| I/O   | Input/Output                         |
| SSMEC | Space Shuttle Main Engine Controller |
| Vdc   | Volts direct current                 |
| PFI   | Power Failure Interrupt              |
| PFS   | Power Failure Sense                  |
| PRI   | Power Recovery Interrupt             |
| BITE  | Built In Test Equipment              |
| PRC   | Pulse Rate Converter                 |
| CIE   | Computer Interface Electronics       |
| A/D   | Analog to Digital                    |
| WDT   | Watch Dog Timer                      |
| IE    | Input Electronics                    |
| OE    | Output Electronics                   |
| MIB   | Master Interconnect Board            |
| BCH   | Bose, Chaudhuri, Hocquenghem         |

|      |                                   |
|------|-----------------------------------|
| VIE  | Vehicle Interface Electronics     |
| RTC  | Real Time Clock                   |
| msec | Millisecond                       |
| PBDN | Power Buss Down                   |
| ac   | Alternating current               |
| PSC  | Power Supply Conditioner          |
| Hz   | Hertz                             |
| Grms | G root-mean-square                |
| F    | Fahrenheit                        |
| EMI  | Electro Magnetic Interference     |
| dB   | Decibels                          |
| psia | Pounds per square inch - absolute |
| EIU  | Engine Interface Unit             |
| R    | Rankin                            |

## TECHNICAL PAPER

### SPACE SHUTTLE MAIN ENGINE CONTROLLER

#### INTRODUCTION

In March 1972, NASA selected the Rocketdyne Division of Rockwell International to design and develop the Space Shuttle Main Engines (SSME) for the reusable Space Shuttle. The development program was managed by NASA/Marshall Space Flight Center (MSFC) and was supported by the various engineering laboratories within the Science and Engineering Directorate. The engine itself is designed to be reusable for 55 missions totaling 7.5 hr of cumulative operating time, and to operate at a variable thrust level commanded by the Orbiter. Engine control could have taken alternate forms such as time sequenced valve control, pressure-ladder sequenced propellant valve control, analog computer control, or digital computer control. A digital computer control concept was selected as the basis of the control system and was designed with the appropriate input-output (control) electronics to interface with the engine hardware. This alternative results in several advantages:

1) Changes in operational sequences and functions were readily accomplished simply by changing computer software programs, thereby avoiding costly and time-consuming hardware redesign, retrofit, reverification, and engine recalibration firing.

2) It provided the flexibility and ease of change needed during the engine research and development phase along with the eventual autonomy and adaptability necessary in a fully operational system.

3) Development schedules were simplified because the hardware design and fabrication proceeded in parallel with software development.

4) A digitally based system provided the fast control response necessary to accomplish thrust level control and maintain a constant fuel/oxidizer mixture ratio over the complete throttle range.

5) It provides the capability of monitoring engine operating conditions and performs various types of safing operations depending on the nature of anomolous or failure conditions detected real-time during flight.

6) A digital system with its associated software is able to perform tests on the engine hardware and self-tests on itself and report any function not performing within specification that might need correcting. Failure detection, isolation, and resolution is more readily accomplished without inpacting other system operations.

7) Operating conditions and component redundancy management results are always readily available to be transmitted, digitally, to the Orbiter and to the ground.

The engine developed for the Space Shuttle represents the most complex high-performance engine ever built. Due to the extremely high operating thrust chamber and turbopump temperatures, pressures, and speeds, very precise monitoring and control of critical engine parameters are of prime importance. Because of the speed and accuracy required in controlling these parameters, the application of a software controlled digital computer was a natural approach.

To reduce the development risk and cost, the Honeywell HDC-601 airborne computer functional organization and logical design was selected as the central processing unit for the SSME control application. This unit, along with specially designed input/output interfacing electronics, power supplies, and appropriate redundancy control electronics, was duplexed and packaged into a unit called the controller.

Since each flight controller is mounted directly on an engine, the environment in which it operates is very severe. Therefore, special emphasis was placed on the mechanical design and packaging techniques of the electronic components and subassemblies. An extensive design verification (qualification) program was instigated and implemented to assure that the controller operates and survives under all the conditions to which it is exposed and for the number of missions for which it is designed.

During the controller development and testing program, various problems and design deficiencies were recognized, analyzed, and corrected. Some were unique because of the nature of the controller design and application, and some were typical of those expected in any electronic package design and development program.

Each of the functional elements comprising the controller is described and discussed in detail. The redundancy configuration employed and the redundancy management concepts, schemes, and techniques utilized are covered. The mechanical design of the controller package, which must withstand the unusual operating environment and the extensive testing to assure controller flight worthiness, is then considered. Finally, operational functions, timelines, and experience are presented.

## CONTROLLER ARCHITECTURE AND ORGANIZATION

The controller serves two basic purposes and functions. First, it monitors and controls the main engine during both normal and emergency conditions; and second, it performs self-tests, diagnostics, and configuration management on itself and other key engine components. In implementing the engine control, checkout, and monitoring requirements, the controller provides the following functions and interfaces:

- 1) Interface with the Orbiter/engine data bus to receive engine commands and transmit data.
- 2) Interface with and provide signal conditioning, multiplexing and analog-to-digital conversion for turbopump and combustion chamber temperature and pressure sensor signals, valve positions, and analog built-in-test signals. Also, provide pulse rate to digital conversion for turbine speed and fuel/oxidizer flow signals and monitor spark igniter signals.

3) Interface with and provide output electronics signals to command servo valves, on/off servoswitches, igniters, and on/off pneumatic valves.

4) Provide built-in test hardware to validate the integrity of the engine hardware and the controller itself.

5) Provide electrical interfacing with redundant vehicle ac power buses and a dc bus used for internal controller heating.

6) Provide connectors and circuitry for ground support equipment to load, alter, and verify memory.

The controller interfaces with the engine, Orbiter, and ground test equipment which enables the controller to perform the above functions as shown in Figure 1. The number of active/total interfaces with each engine or Orbiter element is also indicated in this figure.

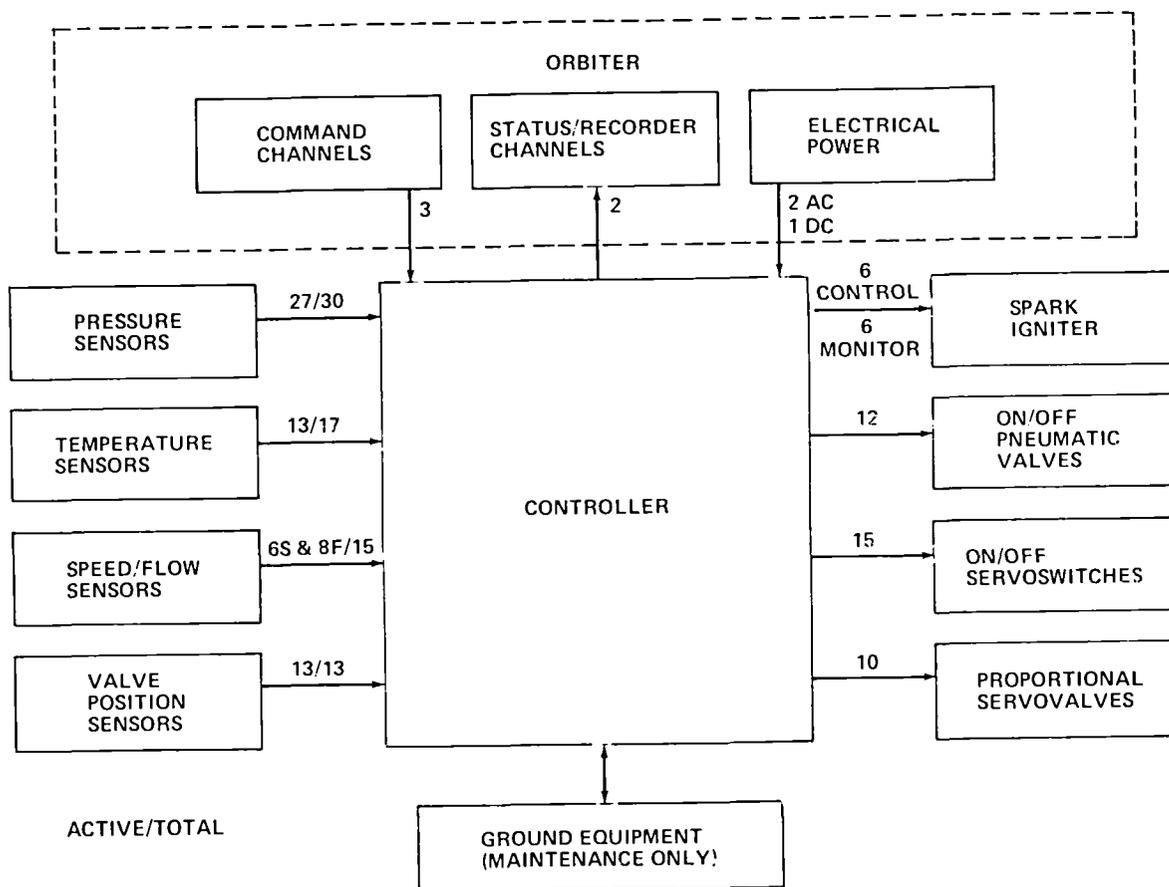


Figure 1. Controller interfaces.

Functionally, the controller can be broken down into the digital computer unit, computer interface electronics, input electronics, output electronics, power supply, and redundancy management control hardware. Operationally, these functions are repeated to

form a redundant channel. Each operational element contained in the controller system is described and discussed following a more detailed treatment of the redundancy scheme employed.

### Redundancy Management

The electrical design criteria listed in the engine Contract End Item (CEI) specification states that "All electrical critical subsystems shall be fail operational after the first failure . . . and fail safe after the second failure." Simply stated, this means that one controller failure will be transparent to the engine and normal engine control can continue. If a second controller failure occurs, the engine would be shut down in an orderly, controlled manner. To satisfy this requirement, the controller was designed with redundant functional channels identified as channel A and channel B, each consisting of input electronics, output electronics, computer interface electronics, central processing unit, and power supply. The cross strapping and redundancy paths which exist within these channels are shown in Figure 2. During normal operation, channel A is the controlling channel, but channel B is powered up and operating in a stand-by mode ready to assume immediate engine control in the event

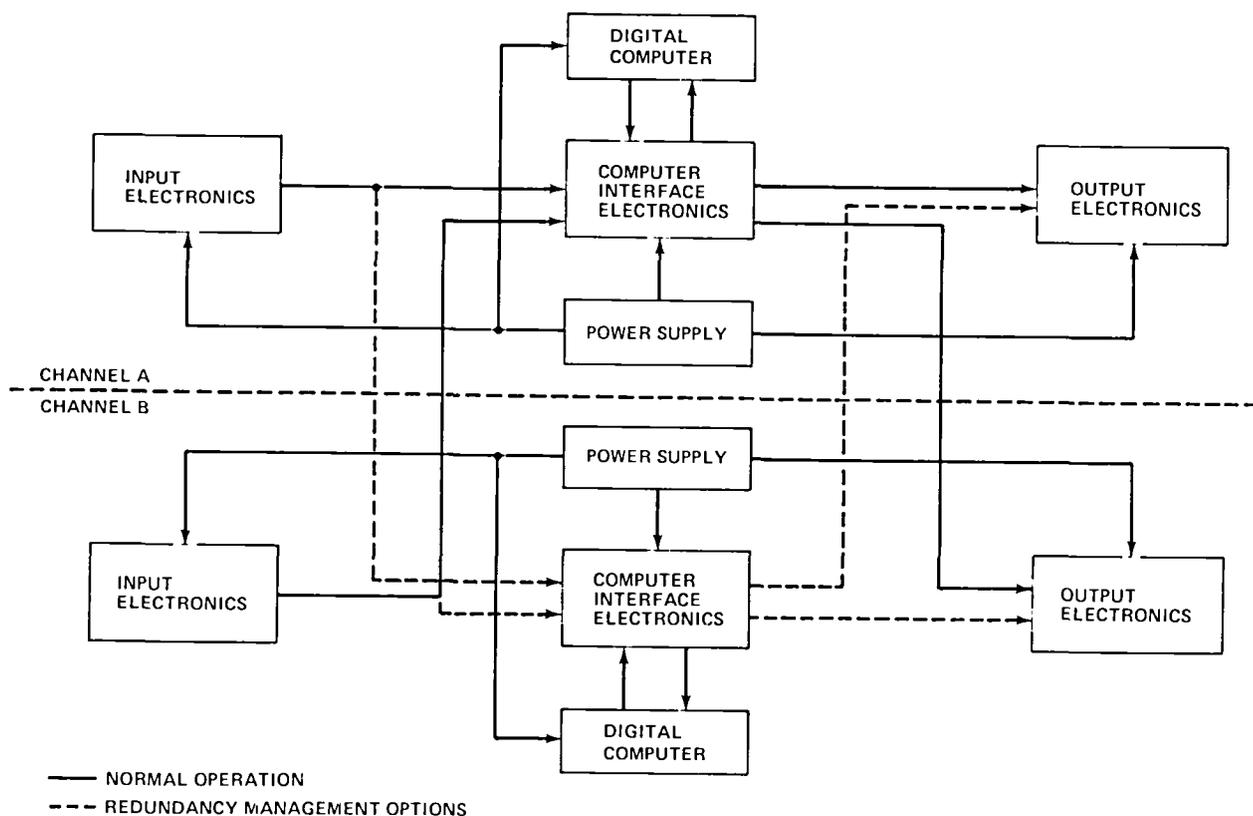


Figure 2. Simplified redundancy diagram.

of a failure of the channel A computer. To maintain this capability, channel B tracks the operating condition of the engine at all times, and monitors the health of the channel A computer. As shown in Figure 2, the power supplies, central processing units, and computer interface electronics are dedicated to their respective channels whereas the input and output electronics are cross-strapped through the computer interface electronics. This level of redundancy and the cross-strapping scheme assures that no electronic single point failure will result in the loss of controller functions, engine shutdown, or unsafe engine operating conditions. This design maximizes the probability of successfully completing a mission in the event of an internal failure. The type cross-strapping which is mechanized in the controller results in a system which is 15 to 20 times more reliable than two simplex channels.

The redundancy management scheme designed into the controller performs the required redundancy action in response to detection of engine/controller failures. This is achieved by very active interaction between hardware and the flight software program. Three distinct areas that can be identified are failure detection, fault isolation, and channel switching. The ability of the controller to detect a failure which results in some engine/controller function being ineffective is accomplished in one of two ways. The first is an interrupt system which is hardware mechanized within the controller and completely autonomous to software operation. Once an interrupt is recognized, however, the software performs an isolation routine to determine what hardware failure caused the interrupt to be generated. The second method by which the controller detects failures is by performing software controlled self-tests of various hardware areas. For example, after a register in the output electronics is loaded with a command, the register contents are read back into memory to confirm a good load. If the command is correct, it is then executed; but if it was loaded incorrectly, appropriate re-try or failure reporting is initiated.

For some cases, failure isolation is achieved merely by the software knowing what piece of hardware it is performing a self-test on. In other cases, as mentioned above, it may be necessary for certain software routines to be performed to isolate a failure.

If a failure is detected in the controlling channel (channel A), the failed module (such as the output electronics) is declared bad and control would be switched to output electronics channel B. The failure of the module is reported by software so the need for hardware repair can be recognized.

Both computers contain the same flight software program. When not in charge, the channel B computer tracks the operation of the channel A computer and is prepared to take control of engine operations if necessary. The channel B computer is prevented from taking control by dual redundant Watch Dog Timers (WDT) in the channel A computer interface electronics. These electronic timers must be reset in a particular sequence each software major cycle (20 msec). Should the channel A computer not properly perform this reset function, the WDT will time-out and place channel B computer in charge. The channel B computer interface electronics also has a set of dual redundant WDT which, if not properly managed will halt the channel B computer. Failure to reset the WDT counters may be due to a hardware failure which makes it impossible to do so, a software decision to intentionally allow the timers to time-out because of a computer detected self-test failure, or a software malfunction such as the program being hung in a tight loop. In any case, control

signals are generated by the WDT circuit and sent to the IE, OE, and VIE to provide for effective transfer of computer control as required. If the failing channel is the only one functioning (i.e., one channel has already failed), the controller hardware and software provide the capability for an orderly and controlled engine shutdown.

### Digital Computer Unit

The SSME controller digital computer unit (DCU) consists of two identical independent, general-purpose, digital computers as shown in Figure 3. Each computer has a self-contained random access memory, arithmetic/control section, and power supply conditioner with the same functional characteristics as the Honeywell HDC-601 and DDP-516 systems. The DCU memories are non-destructive readout (NDRO) plated-wire type. The two computers are capable of simultaneous operation and execution of similar programs. When installed as part of the total SSME controller, one computer functions in an operational on-line mode while the second computer functions in an operational off-line mode. Both computers are electrically and functionally independent of each other, so a failure in one computer does not cause a subsequent failure in any portion of the other.

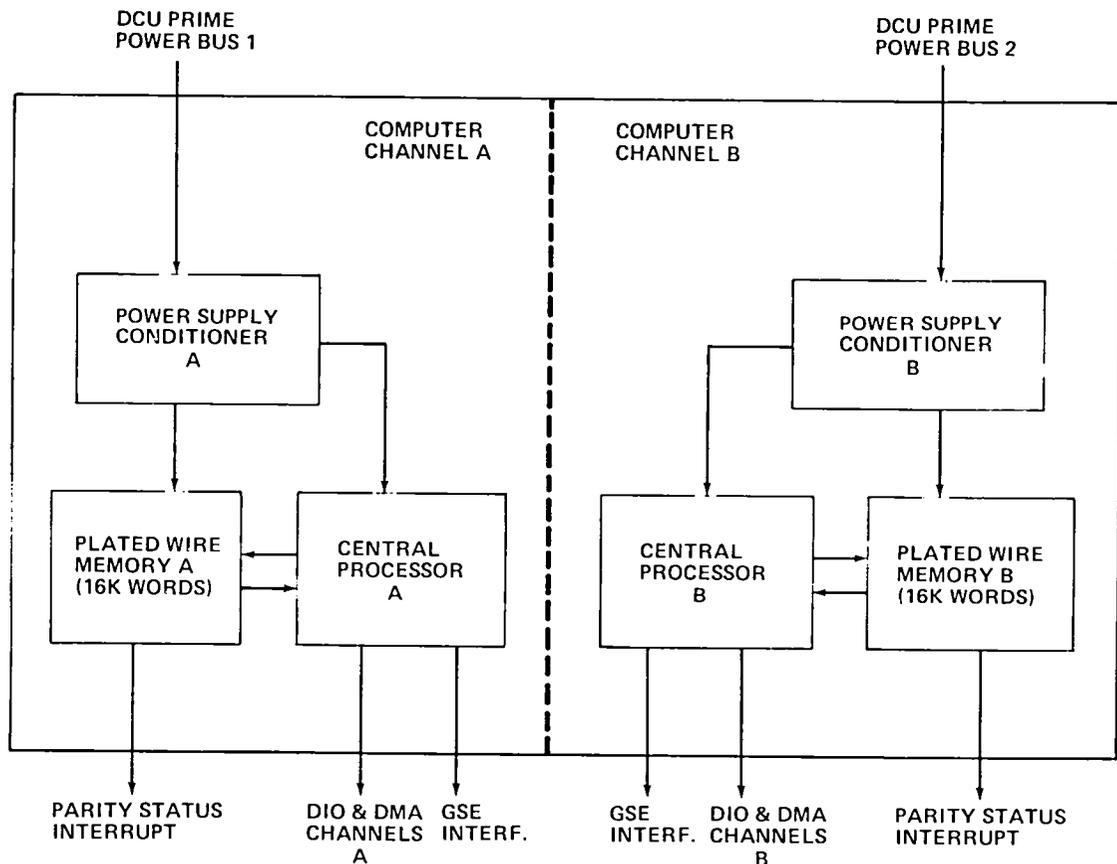


Figure 3. DCU system configuration.

The Central Processor Unit (CPU) design has the following functional characteristics:

- 1) Fully parallel machine organization
- 2) 16-bit word, two's complement representation
- 3) Two full-word arithmetic registers
- 4) One active-circuit index register
- 5) Multilevel indirect address
- 6) Comprehensive instruction repertoire (87 Instructions)
- 7) 1 microsecond memory cycle time
- 8) 390 nanosecond memory access time
- 9) 2 microsecond add time
- 10) 9 microsecond multiply time
- 11) Double precision capability
- 12) 17 external priority interrupts
- 13) Power failure/Recovery interrupts
- 14) DDP-516 software compatibility
- 15) DDP-516 I/O compatibility (DIO channel only)

The DCU is programmed to perform closed-loop control of the Space Shuttle Main Engine, monitor the engine sensors, and run self-tests and check tasks. The DCU executes bi-directional data transfers to/from the I/O electronics of the SSMECA under program or external control. It also interfaces with external ground test equipment (controller checkout console and history memory system).

Each SSMEC-DCU power conditioner is sub-divided into three functional elements as shown in Figure 4. Each module operates off independent power busses from the controller power supply which provides +5 Vdc, +20 Vdc and -6 Vdc nominal operating and logic voltages. Each PSC supplies two regulated supply voltages, +8 Vdc and + Vc, to its associated memory module. The Vc supply is a temperature dependent digit write current source, and the +8 Vdc functions as the positive supply for the word current generator. Both regulator outputs have voltage and current limiting to protect memory components. Five undervoltage sensors in each PSC continuously monitor all three prime power lines

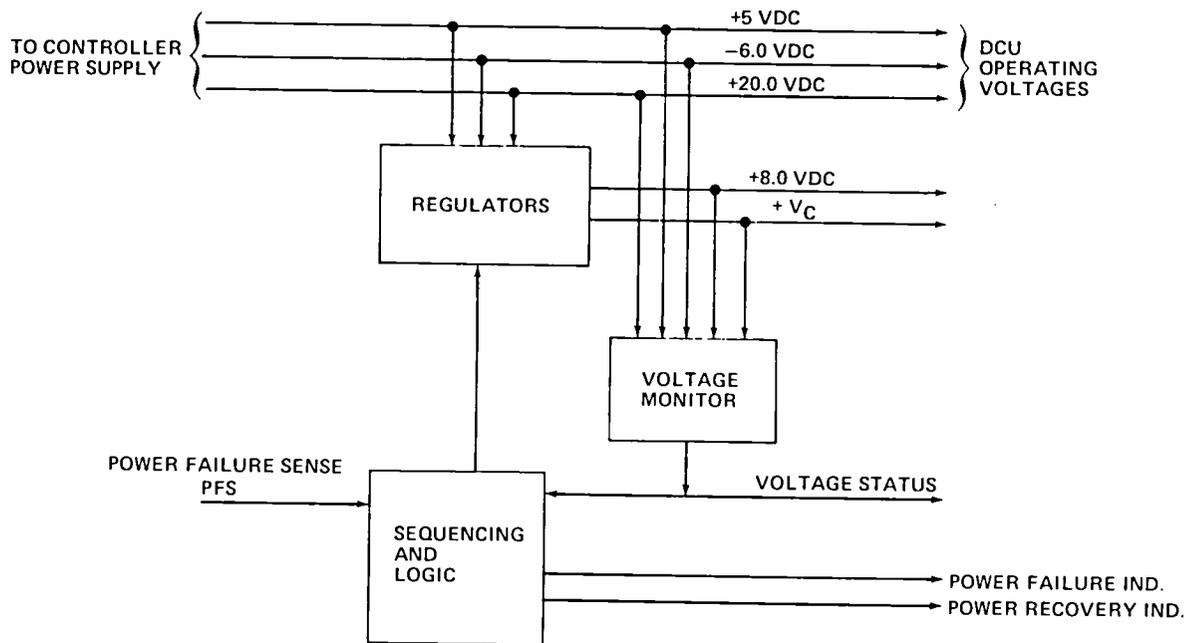


Figure 4. Power supply conditioner.

and the two internally generated memory supply voltages. Voltage monitors provide the necessary signals required by the sequencing logic to correctly effect power sequencing, and together, also determine the state of DCU voltage status signals transmitted to the controller. Each PSC utilizes the signals from the undervoltage monitors and controller to control the sequencing of the DCU for turn-on and turn-off protection of memory data. The PSC provides a power failure interrupts (PFI) signal to the central processor in response to a controller generated power failure sense (PFS) signal. The PFI is generated upon loss of prime power. The PSC provides a power recovery interrupt (PRI) signal to the central processor when all operating voltages are available and have stabilized. A voltage reference in each PSC supplies a known voltage to the undervoltage monitors to which the monitored voltage is compared. The reference also establishes the fixed voltage source from which the V<sub>c</sub> temperature control input is derived. The 5 V undervoltage monitor has built in test equipment (BITE) hardware which, under software control, forces the monitor to an undervoltage condition for testing purposes.

## Memory

A non-destructive-read-out plated wire memory is used in each redundant computer channel. Each channel is designed with a memory capacity of 16,384, 17 bit words and physically consists of two identical half-stack modules. As shown in Figure 5, each memory module consists of four memory boards and a word electronics board interconnected into a common connector base plate. The baseplate is then plugged into a master interconnect board (MIB) pin field when the half-stacks are physically installed into the controller chassis.

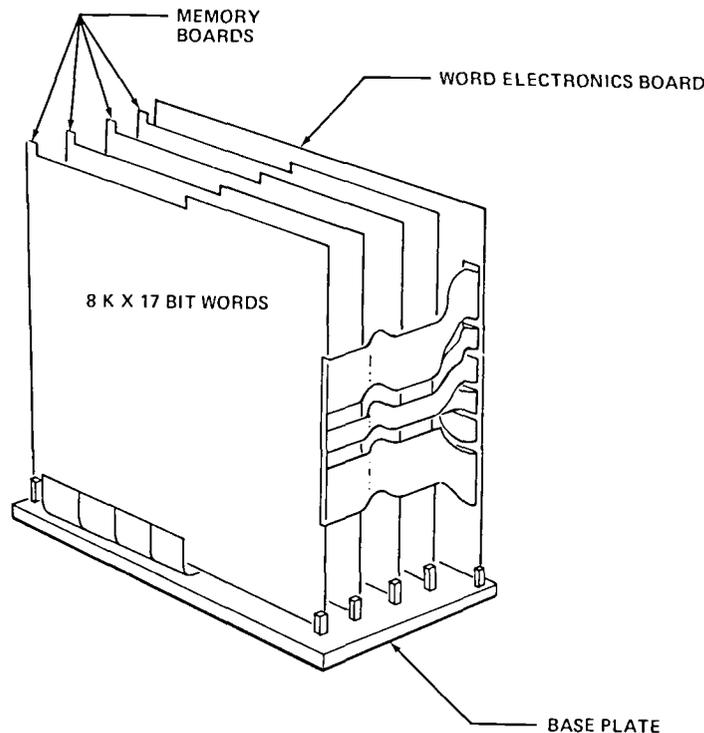


Figure 5. Memory half-stack module.

Physically, as shown in Figure 6, each memory board consists of two memory planes, one on either side of a substrate. Each memory plane is fabricated such that tunnels exist through the length of a portion of the board. The memory storage media, which consists of a 2-mil coupled film plated wire, is formed into a hairpin shape and inserted into the tunnels as shown in Figure 7. The ends of the wires are then soldered to pad areas at one edge of the board, and the pads are interconnected to form longer paths over which data is written. Lying on the memory board surfaces, at right angle to the plated memory wires, are parallel conductors called word straps which are used for memory word selection. When the proper decoding is performed and a word strap is selected, a memory read or write operation can be performed. If a read operation is to be performed, a small word current is passed through the appropriate word strap and the output pulses of the plated wires are sensed by sense amplifiers. The polarity of plated wire pulses, as detected by the sense amplifiers, determines whether "ones" or "zeroes" are read from the 16 bits (plus parity)

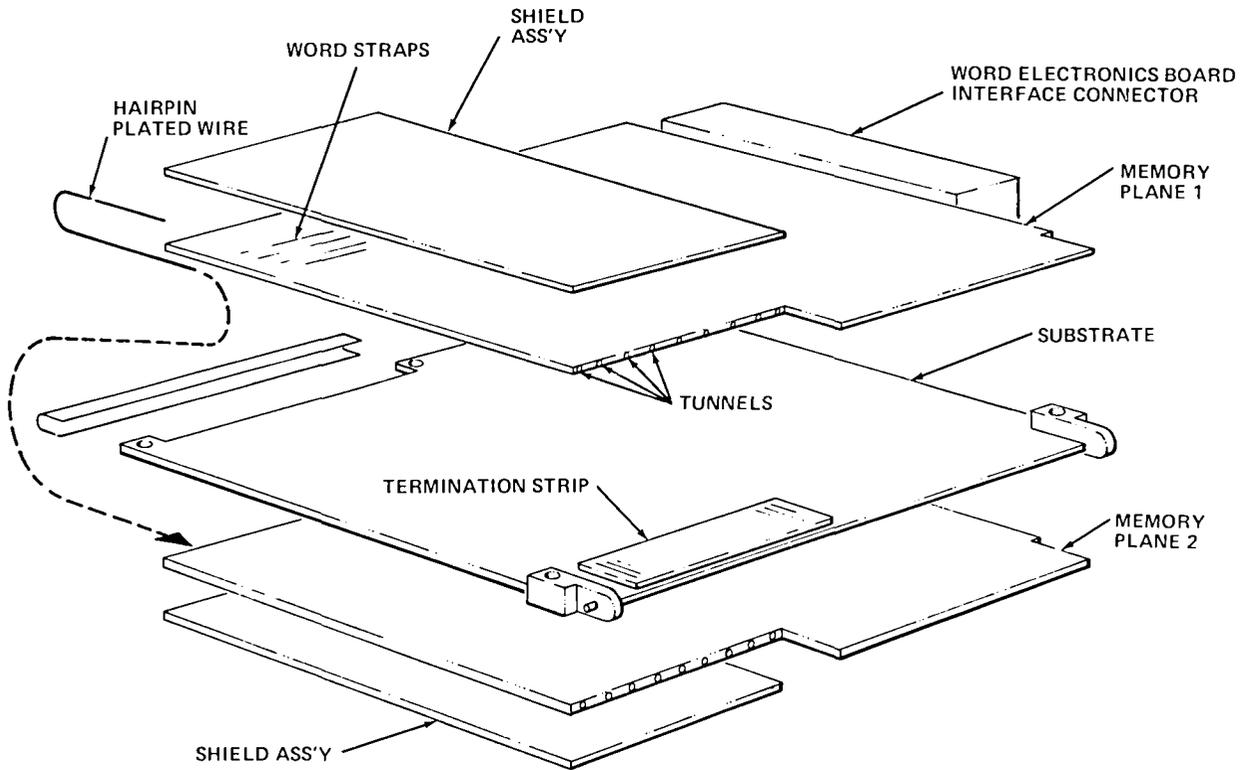


Figure 6. Memory board assembly.

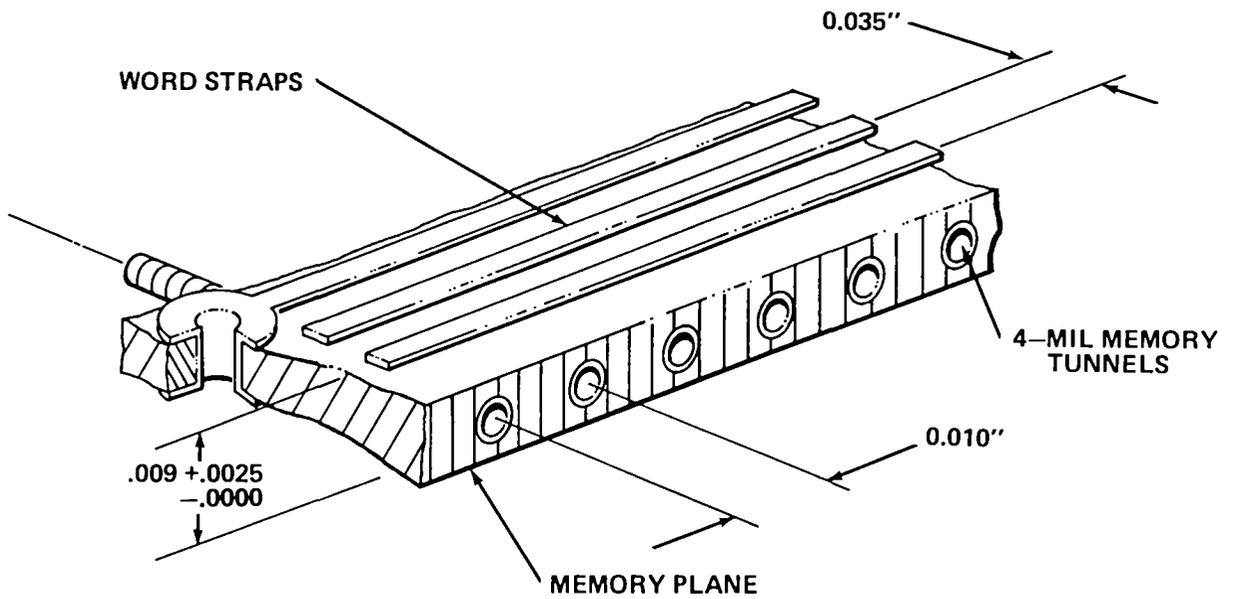


Figure 7. Tunnel structure/memory plane detail.

at a particular memory location. If a write operation is to be performed, a small digit current is passed through the appropriate plated wires at the same time the word current is applied to the word straps. The polarity of the digit current applied to a particular plated wire determines whether a "one" or "zero" is written into that bit position of the 16 bit word. The parity bit, on a write operation, is automatically generated such that an even number of "ones" are written into each memory location. When a memory read operation occurs, the state of the parity bit associated with that particular location is checked. If the correct parity does not exist, an interrupt is generated and appropriate action is initiated. Memory location addressing, digit current signals, and word current signals are generated on the word electronics board of each half-stack. These control and signal lines are then applied to the memory boards where the appropriate memory location is accessed, and the appropriate memory operation is performed.

### Computer Interface Electronics

The block diagram of the computer interface electronics shown in Figure 8 contains the vehicle interface electronics, the computer input/output interface electronics, and the direct memory access control subassemblies.

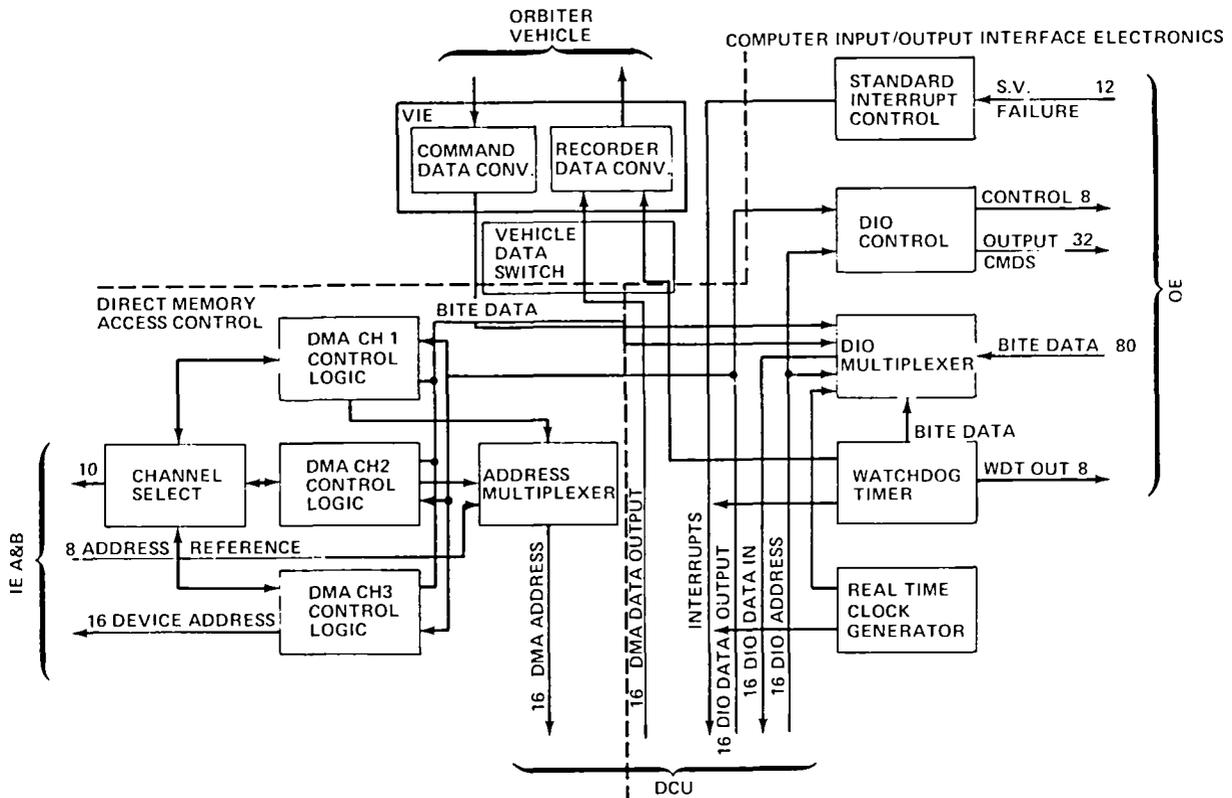


Figure 8. Computer interface electronics.

The vehicle interface electronics (VIE) subassembly consists of a command data converter, a recorder data converter, and a vehicle data switch. Controller commands and memory data words originate at the Shuttle Orbiter and are transmitted over three independent (triple redundant) commands lines. These three identical 16 bit commands are first routed to an engine interface unit (EIU) where they are encoded and subsequently transmitted to the command data converter in the controller. The transmission rate is 1 megabit in the form of a Manchester Bi-Phase (Level) square wave signal. Each transmission from the EIU consists of a total of 31 bits: 15 bits for Bose, Chaudhuri, and Hocquenghem (BCH) encoding and 16 bits for command and/or memory data. The command data converter in the controller receives and decodes the transmission, and detects and rejects error patterns. If hardware checks of correct BCH code, number of bits per word, valid Manchester code, and non-zero word have been satisfied, the transmitted word is then stored in command data converter hardware registers for subsequent DIO transfer into the computer memory. Each of the three commands is verified by an independent command converter in the CIE, and any command or data word which fails any of the hardware tests is interpreted and stored as an all-zero word in its command converter.

All data is transmitted from the controller to the orbiter via serial digital data transfer from the recorder data converter. The dual redundant transmission of data words is at a 1 megabit rate and consists of 16 bits of data plus a parity bit for each data word. A complete data table transmission of 128 words is accomplished in 2.4 msec at a rate of one table every 40 msec. Each data table contains sensor parameter values, valve positions, command data, and failure data. The data table is transmitted as a Manchester bi-phase (level) signal.

The vehicle data table transmitted to the Orbiter is supplied by either of the dual redundant digital computer units and is fetched from memory by direct memory access control. The vehicle data switch, which is controlled by the redundancy management scheme, determines whether DCU A or DCU B data is actually selected for transmission. A more thorough description of the redundancy capability and operation is described in a later section.

The computer input/output interface electronics subassembly consists of a watch-dog timer, a real-time clock, standard interrupt control, direct input/output control, and a direct input/output multiplexer, all of which are shown in Figure 8. A dual-redundant watch-dog timer (WDT) in the input/output electronics is incorporated in each redundant computer interface electronics channel to indicate the performance status of each DCU channel to the other. When DCU channel A fails, its WDT status signal is used to transfer control to DCU channel B. Either redundant watch-dog timer in a DCU channel can signal failure of that channel (to provide failsafe monitoring of each DCU channel).

Each watch-dog timer times out in  $18 \pm 3$  msec if not retriggered by the DCU. Retriggering occurs after 10 msec, and each timer is retriggerable by a separate control signal command from the DCU. One watch-dog timer is incremented by the real-time clock, and the other by a clock from the output electronics. The mechanization takes into account all frequency and skew variations between the two clocks to provide failsafe switching and periodic testing. To inhibit the failure state during checkout, inputs from the Ground Support Equipment (GSE) are provided to maintain the watch-dog timers in the "on" state without DCU retrigger pulses.

Provisions are also made to initialize each watch-dog timer to the timed-out state when power is turned on initially and after recovery from an input power bus transient. To initialize the channel A watch-dog timer, a control signal from DCU channel A and a control signal from output electronics channel A are used. Similarly, the channel B watch-dog timer is initialized using signals from the channel B output electronics and DCU.

A real-time clock (RTC) is provided for each computer input/output electronics channel as shown in Figure 8. The RTC, which uses a DCU clock and provides a timing reference interrupt at intervals of 5 msec, provides a signal to increment the counters of one watch-dog timer as described above. The software has the capability to read the outputs of the real-time clock to monitor clock operation. Each RTC consists of a 13-bit counter driven by a 1 MHz clock. The counter starting value is 4999 and is counted down at a 1 MHz rate. At a count of zero the 5 msec interrupt signal is generated, and the counter resets itself to a value of 4999.

As indicated in Figure 8, each CIE contains the necessary hardware to provide a standard interrupt signal to its DCU when a servoactuator failure occurs in either the A or B channel monitor circuits. Output signals from the ten actuator monitors are multiplexed together to generate the standard interrupt. A mask register exists in the standard interrupt control which can be used to mask off (block) all inputs or used to poll the monitors to determine which actuator is failing. If polling is to be performed, the status of the servoactuator monitor lines is read as one of the digital self-test words loaded into memory.

Two methods exist within the controller to control the flow of data into and from memory. One method is strictly under the management of the flight software and is called direct input/output (DIO). The direct input/output (DIO) control shown in Figure 8 provides signals to control the flow of data into and out of the DCU via the DIO data channel. The DIO channel consists of address decoding logic which decodes the DIO address bus to determine which device to select, and strobe logic to provide control signals needed for transfer operation throughout the controller. It is through this path that data is transferred to the output electronics for subsequent engine igniter and valve commands.

The DIO multiplexer is the interface through which the software controlled data input to the DCU is passed. From DIO address lines, appropriate control signals are decoded which select Orbiter commands, RTC data, servoactuator interrupt status or various BITE data to be placed on the DIO data input bus. A total of 16 digital self-test words may be accessed and read into computer memory by this means.

The second method used to control the flow of data to and from memory is by direct memory access (DMA). As the name implies, this method allows direct access to memory to achieve high rate data transfer without involving the central processing unit. When a DMA read (data output to the Orbiter) or DMA write (bringing sensor data into memory) request is recognized by the processor, it pauses and relinquishes the next memory cycle to the DMA control hardware so that the requested operation can be performed. Hardware registers are loaded with a starting address and the number of sequential addresses

to be written into or read from. After the DMA control hardware receives the initiate pulse, it provides the necessary control signals for proper DMA operation. After each read or write operation, the address register is incremented and the range register is decremented. When the range value has counted down, the DMA cycle is terminated; and control is relinquished to normal software controlled operations.

The direct memory access (DMA) control subassembly of the CIE shown in Figure 8 consists of three channels. Control channels 1 and 2, which are actively redundant, control the interface between the memory and the recorder data transmission interface, and control channel 3 inputs the A/D converter and the pulse rate converter data. Each DMA control logic block contains memory address and range counters which are loaded under software control. The range and address counters located in channel 1 and channel 2 control logic are used for DMA operation which control computer memory outputs to data recorders A and B, respectively; and range and address counters in channel 3 control logic are used for DMA operations which control DMA sensor and parameter inputs.

A priority structure determines which of the three channels has access to the memory. Channel 1 has highest priority, channel 2 has next highest, and channel 3 has lowest priority. Once a channel has completed its operation, the priority structure determines which channel next has access to the memory. Channels 1 and 2 control the DMA during the time that a data word is being transferred to the vehicle interface electronics, but control of the DMA is released while this data is being transferred to the data transmission interface. Channel 3 address and range counters are loaded by the computer to sample and convert a sequence of analog sensor and parameter input signals, but control the DMA only long enough to transfer A/D converter outputs to the memory and initiate a new conversion cycle. Also, channel 3 samples the pulse rate converters in a sequential manner, once it has received a control pulse from the DIO Control, and transfers the data to the memory. This transfer is performed whenever channel 1 and channel 2 are not in control or are not requesting control of the DMA control electronics.

The time required for a DMA output from channels 1 and 2 is 19  $\mu$ sec per word. After the channel 3 address and range counters have been loaded and the initiate pulse issued, the time required for a DMA input through the A/D converter into memory is approximately 106  $\mu$ sec. The time for a DMA input through the pulse rate converter interface is 3.0  $\mu$ sec.

A checking circuit is provided in the Channel 3 DMA logic to monitor address bits 3 through 8 to detect errors which would otherwise cause undetected memory alterations during DMA channel 3 storage of data into memory. If the configuration of bits 3 through 8 would result in data being placed in memory outside of the data storage area, an interrupt is prohibited from being generated. In addition, the checker circuit is tested to verify its ability to detect DMA channel 3 address errors. Control signals initiate the test of the address checker.

## Input Electronics

The input electronics (IE) acquires analog data, conditions it, converts it to digital data, and transfers the digital data to the DCUs. Figure 9 shows a block diagram of the input electronics which consists of the following major elements and functions:

- 1) Pulse rate converters
- 2) Temperature and pressure sensor electronics
- 3) Low level and high level multiplexers
- 4) Analog-to-digital converter
- 5) DMA input multiplexer
- 6) Command select switch.

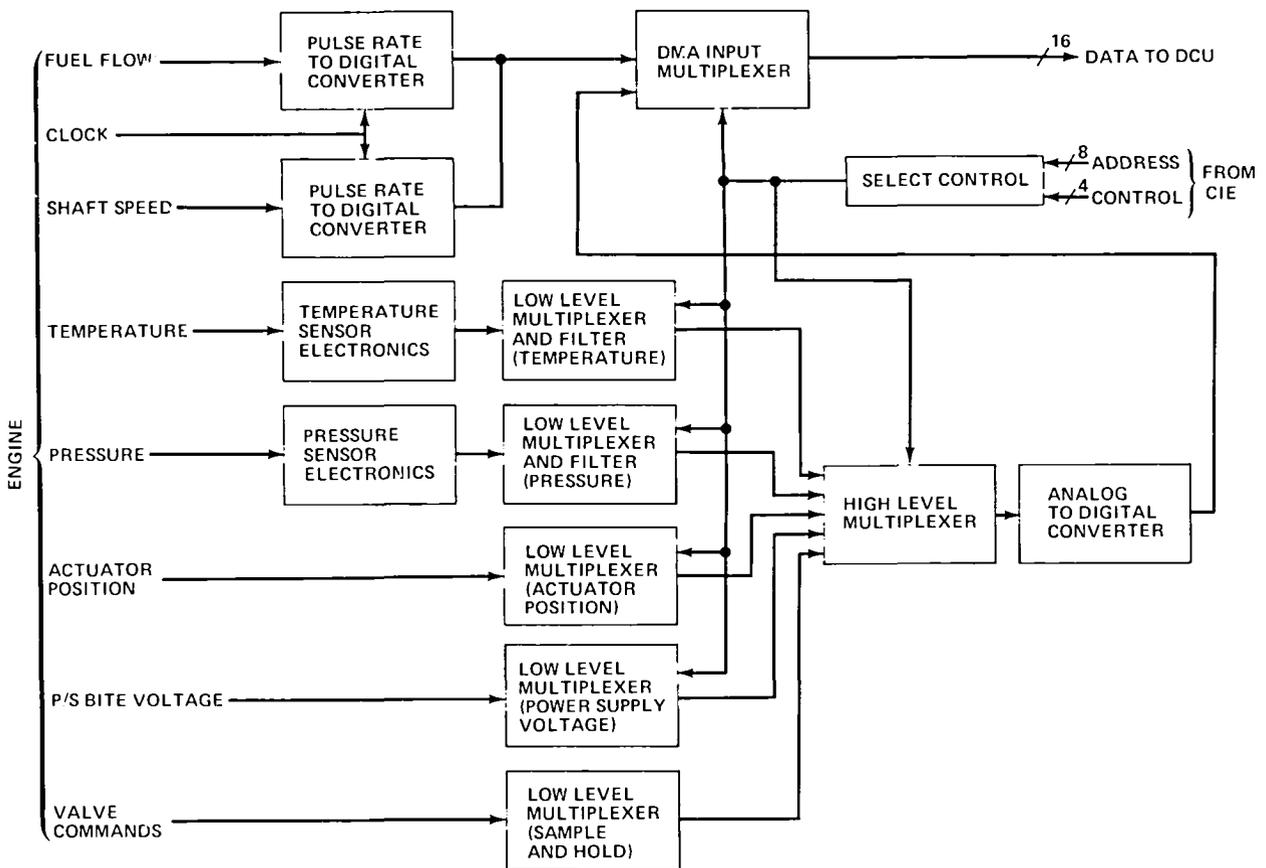


Figure 9. Input electronics.

Inputs to the pulse rate converter (PRC) circuits are pulse trains which represent the shaft speed of engine turbopumps and flowrate of propellants. As the shafts of the pumps revolve, pulses are induced into signal lines attached to the controller. Using these pulses, the PRC circuitry starts and stops a counter which is incrementing at a 1.5 MHz rate. The output of the counter is a 16 bit digital word whose value is inversely proportional to the speed and flowrate input. The resulting digital value is then fed to the DMA input multiplexer and subsequently stored in memory as previously explained. Appropriate control signals are generated to reset the PRC circuitry before it begins to count, to indicate when the conversion is complete, and to indicate when data is ready to be read. Each speed and flow sensor contains dual redundant output windings. The controller performs check-out of these sensors by exciting one of the windings with a 500 Hz test signal and monitoring the output, produced by inductive coupling, in the other sensor output winding.

Temperatures on the main engine are in the cryogenic and hot gas range (37°R to 1700°R) and are sensed by thermisters placed at various critical positions on the engine. The thermister outputs are supplied to the input electronics of the controller where they are used as the fourth leg of resistance bridges. The other three legs of the bridges are contained within the input electronics of the controller. There are a total of 17 temperature bridges within the controller.

Pressures monitored by the controller vary from the high pressure of the oxidizer turbopump (5200 psia) to the internal pressure of the controller itself (23 psia). All engine pressures are sensed by strain gauge transducers (bridge circuits) located throughout the engine hardware. Redundant measurements, supplied by redundant sensors, are available to the controller for the most critical parameters. There are a total of 32 pressure bridge input circuits within the controller.

The temperature and pressure input circuits contain calibration input signals which are multiplexed into memory with the temperature and pressure sensor signals. These calibration inputs are used as part of in-flight BITE for monitoring circuit integrity. The input electronics of the controller also contain provisions to individually connect a resistive load across one leg of each temperature and pressure sensor bridge. This produces a simulated sensor output of 80 percent and 50 percent full scale for the pressure and temperature sensors, respectively, and is used to check out the sensors and circuit paths. All temperature and pressure sensor bridge outputs are filtered and then routed to low level multiplexers, one dedicated to pressures and one to temperatures.

In addition to the temperature and pressure low level multiplexers, the input electronics also contain multiplexers for various controller operational and control voltages, valve commands, and engine valve positions. The outputs of all low level multiplexers are amplified, multiplexed by a high level multiplexer, and applied to an analog-to-digital converter.

The analog-to-digital conversion is initiated by a start conversion signal from the computer interface electronics. This signal is generated after the appropriate address lines have been decoded by the select control logic to specify the desired sensor input (i.e., a temperature, pressure, PRC, voltage, or valve input). The total analog-to-digital conversion time, from receipt of an analog device address command until the data has been transmitted

to memory, is less than 106  $\mu$ sec. When a conversion is complete, the A/D converter retains the converted signal until reset by another start conversion pulse. Although the DCU operates on a 16 bit word format, all analog inputs are converted to 10 bit digital words. The six low order bits in the word format are unused, remain fixed, and do not contribute any signal to the A/D converted value. The 10 bit converted value represents an analog value between -5.0024 and +4.9926 Vdc, with negative numbers represented in two's complement form. If the analog input value exceeds these limits, the digital output is held at full scale. The controller has provisions for confirming that there are no "stuck" bits in the A/D converter and that conversion accuracies are within specified tolerances.

All PRC digital data and the A/D converter output go to a DMA Input Multiplexer. Device address lines from the computer interface electronics are decoded and used as control lines for the multiplexer to select the appropriate digital word to be input to memory by DMA operation. If both of the dual redundant controller channels are operational, the address lines which are decoded to select sensor data are selected from the channel A computer interface electronics. If, however, the channel A DCU or CIE has failed, the command select switch will select address lines from CIE channel B to control sensor data input. Watch-dog timer signals (discussed in the redundancy management section) are used by the command select switch to actually control which address source is utilized.

### Output Electronics

The output electronics (OE) shown in Figure 10 receives digital commands from the CIE and converts them into signals suitable to operate the control elements of the engine such as propellant valve servoactuators and servoswitches, solenoid valves, and spark igniters. Like the input electronics, the OE is divided into channel A and channel B which are redundant and independent of each other. Active redundancy is predominantly used except for the closed loop position control of the propellant valve servoactuators. Channel B position control electronics are selected for control by the operational program after a detected position control failure while channel A electronics were in control.

Each OE channel is capable of receiving commands from either CIE. Command selection is determined by the redundant watch-dog timer status signals provided by the channel A CIE such that both OE channels are always controlled by the "in charge" CIE. Outputs from each channel to the engine on-off devices (igniters, servoswitches, solenoid valves) can be deactivated by the flight software under specified conditions. Some outputs from both channels are automatically deactivated when both DCUs are inoperative. The operational status of the output electronics is continuously monitored by the program in the "in charge" DCU by the following procedure:

- 1) The correct receipt of a digital command is verified before the implementation of that command is allowed.
- 2) The correct update of the on-off registers which store on-off device commands is verified.

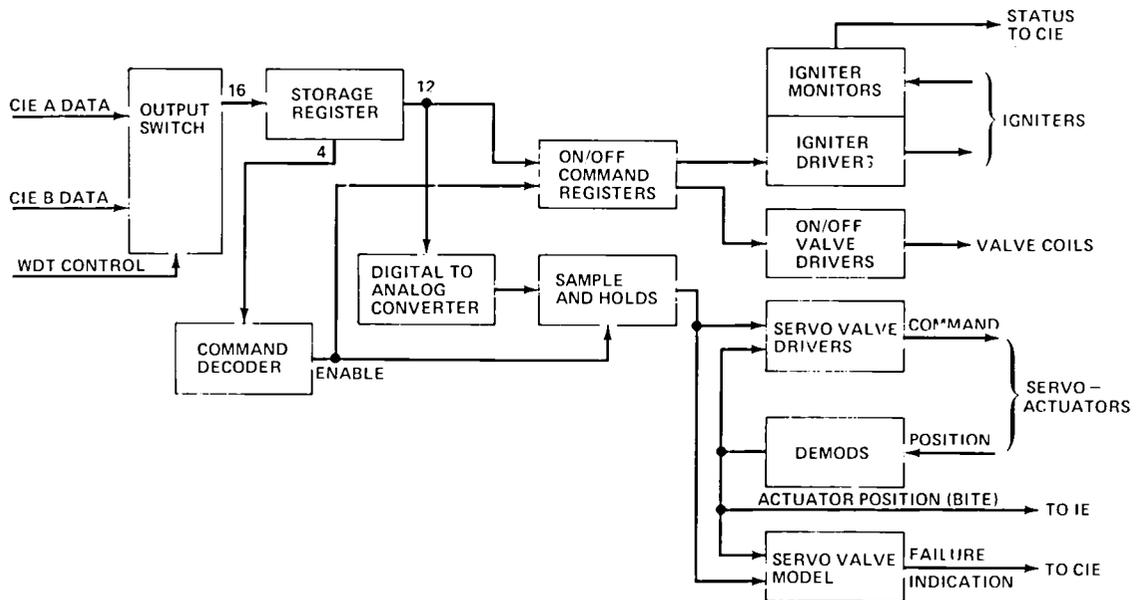


Figure 10. Output electronics.

- 3) Each servoactuator position command is verified for correctness just after it is converted into analog form.
- 4) Status of the on-off devices is periodically monitored.
- 5) Position sensor excitation supply output is periodically monitored.
- 6) Each servoactuator performance is continuously monitored by redundant hardware models and failure detectors. An out-of-tolerance condition is indicated to the flight software by an interrupt request.

Each OE channel also provides excitation for the corresponding valve position transducers of the engine. The following paragraphs describe the basic elements of the output electronics shown in Figure 10. The output switch and storage register accepts 16 bit control commands from each computer via their respective CIE. The WDT control signals from CIE channel A controls the output switch such that the controlling DCU/CIE has access to, and loads, the storage register. Regardless of which DCU/CIE is in control, both computers can perform the monitoring functions associated with the output electronics, for example, performing a DIO input (BITE data) of the storage register, on/off registers, etc. The storage register is 16 bits long and provides temporary storage for control commands before their transmission to selected devices.

The command decoder receives the four least significant bits of the command word from the storage register and decodes them to select the device for which the command is intended. In addition, the decoder is used for test purposes and for passing information from the controlling computer to the computer in standby.

There are two 12 bit registers, in each OE channel, designated as ON/OFF command registers. Their purpose is to provide storage for commands to ON/OFF devices such as solenoid valve drivers, igniters, servo-switch drivers, checkout logic, etc. If the command decoder determines that an ON/OFF command is to be issued, it controls the application of the drive signal from the ON/OFF register to the appropriate device.

The controller supplies both the operating voltage and command signal to excite the engine igniters. If an appropriate word is loaded into the ON/OFF command register, the command decoder allows the igniter energize command to be issued. Each OE channel has drive circuits for the engine preburner and the main combustion chamber igniters. The main combustion chamber, fuel preburner, and oxidizer preburner each have dual redundant igniters, one controlled by channel A OE and one by channel B OE. To initiate an engine firing, both controller output electronics channels issue the energize igniters command. If one igniter fails, the redundant igniter, controlled by the other channel of the controller, generates ignition. When an igniter is firing, it echoes a pulse train back to the controller output electronics. Six igniter monitor circuits within the controller (three in each OE) test the pulse train for correct frequency and amplitude. If the correct criterion is met, individual discrete indications are loaded into computer memory so that software logic can confirm the igniters are functioning properly.

The ON/OFF valve drivers provide commands to operate pneumatic solenoid valve coils and servoswitches. Inputs to the drivers are from bits in the ON/OFF command register and are controlled by the command decoder. The status of the individual drivers is included in the BITE self-test words of the ON/OFF registers and is read under DIO control. In channel B the pneumatic solenoid drivers are the energize/hold type which provide one voltage (+36 Vdc) for energize and a lower voltage (+14.5 Vdc) for holding the valves. In channel A the +36 Vdc source is used for both energizing and holding the pneumatic valves, but the current level is switched. Switching of the voltage and current levels is controlled by high/low power switches which are in turn controlled by the ON/OFF command register. A test signal, which indicates whether a valve is in the energized or hold state, is supplied to the input electronics for A/D conversion. Monitoring this signal by software permits detection of a condition where the energize/hold condition of a valve is not in the state it was commanded to.

When an engine servovalve is to be commanded, a digital value is loaded into the 12 most significant bits of the storage register. The four least significant bits, as discussed earlier, are used by the command decoder to determine which of the five valves is to receive the command. After the contents of the storage register is read back to determine that it has been loaded correctly, the 12 bits are applied to the Digital to Analog (D/A) converter to be converted to an analog drive voltage suitable for driving the sample and hold circuits. The binary input is converted into a dc voltage within 10  $\mu$ sec with a conversion accuracy of  $\pm 0.2$  percent full scale output. The full scale output range is from -6.0 to +6.0 Vdc and corresponds to a 0 percent to 100 percent valve position command. After the conversion is complete, the dc analog voltage is applied to a sample and hold circuit which "holds" the analog signal and provides the servovalve driver with a continuous input signal. The application of the D/A voltage to a particular sample and hold circuit is software controlled and exists for a minimum of 80  $\mu$ sec before the next sample and hold circuit is loaded. The output of a sample and hold circuit achieves a final value of 99.9 percent of the commanded

value in less than 300  $\mu$ sec and, in addition to being applied to the valve drivers, is routed back to the input electronics to be converted by the A/D converter and read into memory. If the valve command is not of the correct magnitude, appropriate failure response is initiated.

Each of the five engine servovalves supplies a position indication to the controller. This position feedback is demodulated and supplied to both the servovalve driver and a servovalve model in the output electronics. Each servovalve driver sums the command it receives from the associated sample and hold circuit with the demodulated valve feedback signal, and supplies a servovalve drive current proportional to the sum of the two.

Five independent circuits are provided in each of the controller output electronics channels to model or simulate the five engine propellant valves. As with the servovalve drivers, each model receives the appropriate sample and hold valve command and the corresponding demodulated valve position. A comparison is made between the actual valve position and a simulated position from the actuator model. A hardware interrupt is generated when the difference exceeds a specified percent of full scale position. The trip level of the channel A monitors is equivalent to  $\pm 6$  percent of full scale, whereas the trip level of the channel B actuator monitors is equivalent to  $\pm 10$  percent of full scale. The larger trip level in channel B provides for actuator position errors which may occur when switching from controller channel A to channel B during a failure condition. The actuator model and failure monitor is mechanized in the same manner for all actuators.

### **Power Supply Electronics**

The Power Supply Electronics converts vehicle supplied electrical power into the individual voltages required by the controller. The power supply electronics receives electrical power from the Orbiter via dual redundant 115/200 V, 3 phase, 400 Hz, wye-connected power circuits. Each power bus is dedicated to a channel within the controller and may be individually switched on or off from switches in the Orbiter cockpit to verify redundancy within the controller. If a power supply fails, all subassemblies associated with that channel, i.e., input electronics, computer interface electronics, central processing unit, and output electronics, become inoperable. A block diagram of the power supply system is shown in Figure 11.

The power supply electromagnetic interference (EMI) assembly, along with various distributed filters within the power supply, provides the necessary filtering within the controller. This allows proper controller operation without being susceptible to vehicle EMI and without transmitting interference to the Orbiter power system. The EMI filter assembly utilizes a combination of L-R-C series/shunt filter elements to attenuate power bus switching transients from the controller to the Orbiter and from the Orbiter to the controller.

After being filtered, the power bus input is applied to an input assembly whose primary purpose is to monitor and detect loss of input power or abnormal input power. If either of these cases occurs, a power failure sense (PFS) signal is generated which in turn



generates a power failure interrupt to the computer used in that channel. This interrupt forces an orderly shutdown of the memory write currents and prevents memory alterations because of out-of-specification operating voltages. The PFS signal gives sufficient advance warning (110  $\mu$ sec) of an impending DCU failure to allow the software to perform the appropriate housekeeping routines prior to shutdown. In addition to the PFS signal, the PFS circuit issues a Power Bus Down (PBDN) signal to the alternate computer to inform it of the power supply status. This information enables the alternate computer to determine the usability of the input and output electronics channels. In the input assembly, the 115 V input is also applied to a monitor transformer. The output of the monitor transformer is rectified, filtered, and supplied to the input electronics for A/D conversion. The resulting digital value is input to memory by DMA operation and allows a real-time monitor of the input bus voltage amplitude.

All of the controller operating voltages are generated within the output assembly of the power supply. Some voltages are generated, filtered, and used raw, but the more critical voltages are regulated. In addition to being distributed to the appropriate circuits, these voltages are supplied to the input electronics where they are converted by the A/D converter and stored in memory by DMA operation.

A thermistor located in the channel A power supply senses the controller internal temperature and controls the controller heater electronics. The heater electronics controls the application and removal of a vehicle supplied +28 V bus to the controller heater element. This circuit is active only during non-operating in-flight conditions and is used to maintain the minimum temperature of the controller above a specified value. This function exists in the channel A power supply and is non-redundant. BITE data is available to the DIO input bus to convey the operational status of the heater.

## PACKAGING

Since the controllers are designed to be mounted directly on the Space Shuttle main engines, they are required to withstand a very harsh environment. With this in mind, a great deal of emphasis was placed on the mechanical design and packaging technique. As can be seen in Figure 12, the main components of the controller chassis are the inboard and outboard covers, the inboard and outboard cases, and the inboard and outboard master interconnect boards (MIB). The cases are machined from an aluminum alloy and are compartmentalized to hold the printed circuit cards and subassemblies. Pin fins are machined on the outside of the cases and inboard cover to conduct heat out of the box and give the case more rigidity. The outboard cover contains 23 connectors and is the electrical interface with the engine, Orbiter, and with ground support equipment. Three connectors on the end of the inboard case accept power from the vehicle power system for subsequent conversion to the required controller operating voltages.

The outboard MIB is the primary means by which interconnections between outboard printed circuit cards are made. The MIB itself is approximately 12  $\times$  18 in. in size and is populated with approximately 9,000 interconnect sockets. Interconnection between

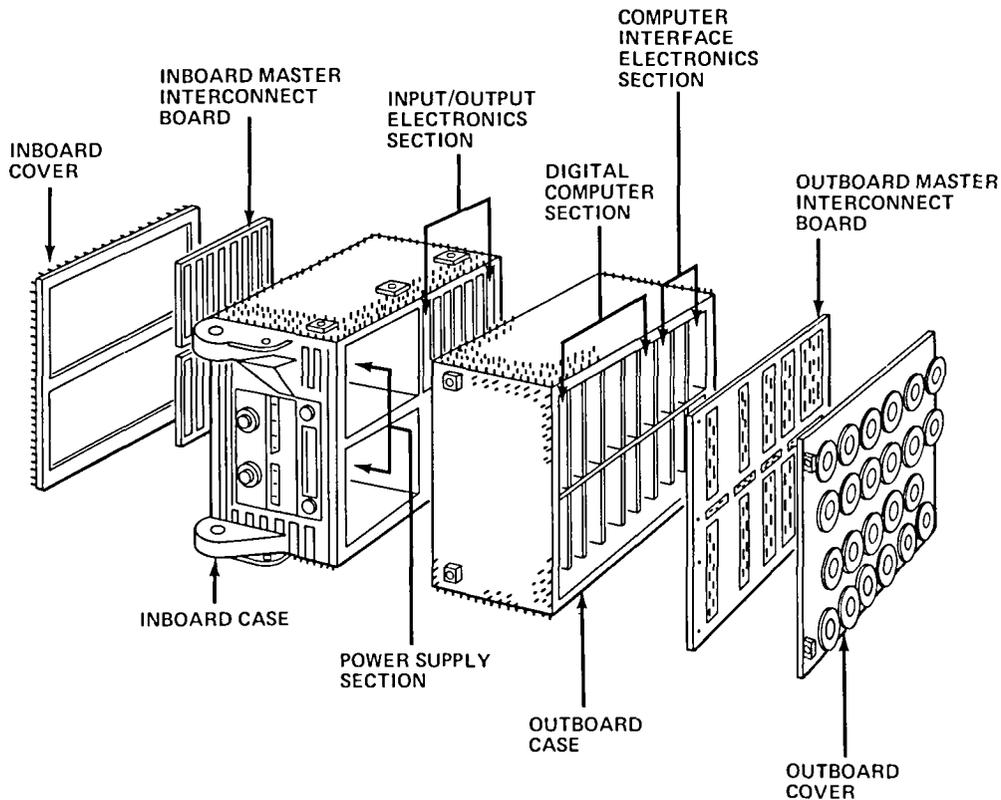


Figure 12. SSME controller.

the printed circuit cards is accomplished on one side of the MIB by stitch welding (resistance welding) teflon coated nickel wire from socket head to socket head as required. Each welded joint is tested to confirm that a reliable bond has taken place. A room temperature vulcanizing (RTV) compound is then applied as "stringers" across the mass of stitch welded wires. This forms a more rigid interconnect system which dampens the effect of vibration and prevents open circuits due to broken wire. After the stitch weld operation is completed and checked by DITMCO, the MIB is installed in the outboard case and the cards are installed.

Each chassis compartment, other than those in which subassemblies are installed, is designed to hold two printed circuit cards, foam grids, and foam wedges as shown in Figure 13. The foam grids are wrapped with an aluminum foil, which serves to transfer heat from the cards to the chassis, and are attached to the cards. Foam wedges are installed against the cards on the opposite side from the foam grids, and the cards are then inserted into the compartments and plugged into the MIB sockets on the opposite side of the MIB from the stitch welds. Between these wedges is installed a "loading wedge" whose purpose is to press the foil-wrapped grids firmly against the chassis wall and to retain the cards during vibration.

Interconnection between the inboard and outboard sections is accomplished by flat cable harnesses, which are plugged into connectors along the edges of the MIBs and routed to the forward end of the chassis where they pass between the two cases. In some instances the total signal paths approach 4 ft in length.

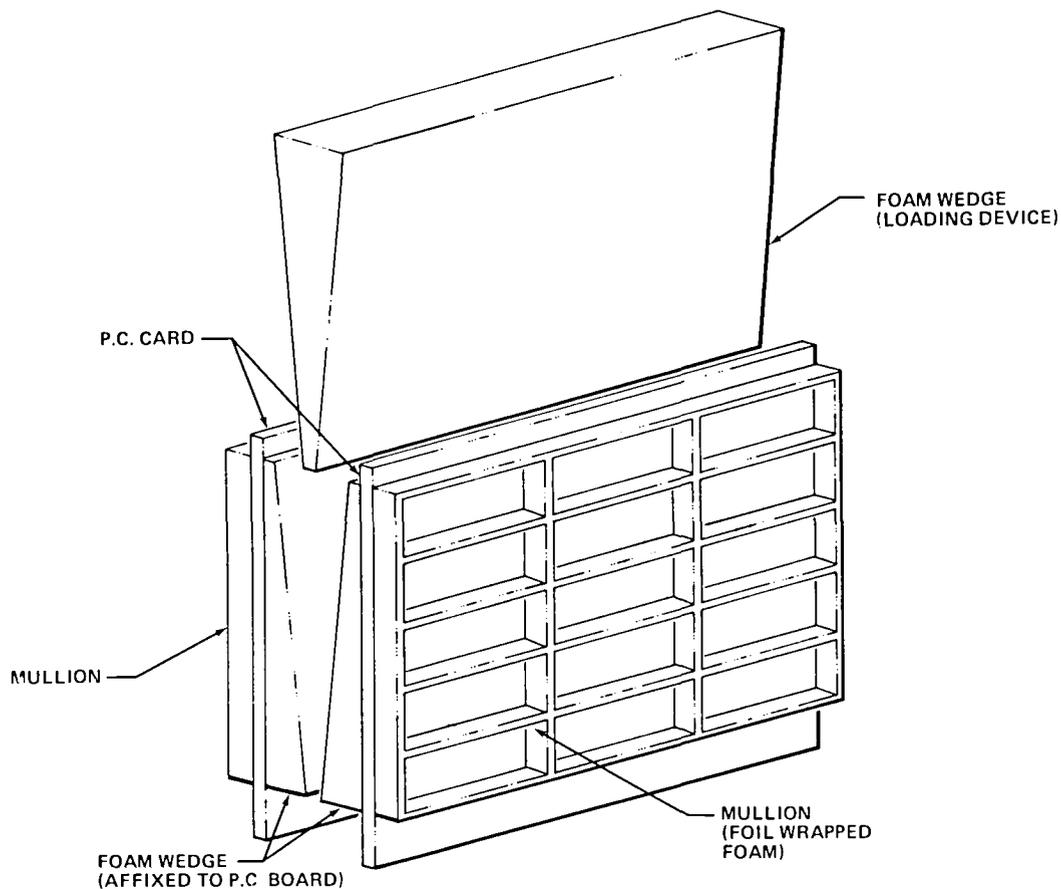


Figure 13. PC board retention design.

The inboard case and MIB are built and assembled similarly to the outboard. The major difference between the MIB's is that the inboard is smaller than the outboard. It is approximately 12 X 12 in. in size and contains over 4,000 interconnect contacts.

The inboard MIB is smaller than the outboard because the power supplies, which are physically located in the inboard chassis, are not required to be plugged directly into the MIB. Excluding the memory and power supply subassemblies, there are 72 printed circuit cards that make up the controller electronics. The total number of piece parts in the controller exceeds 12,000, of which over 3,000 are integrated circuits.

## TESTING

Controller testing is performed at various levels of fabrication with many different test objectives in view. The goal of this test activity as a whole, however, is to detect, recognize, and correct problems and failures as early as possible into the design, assembly, and test flow, thereby saving much redesign, disassembly, rework, and retest time. The major areas of test discussed are:

- 1) Controller qualification testing
- 2) Controller acceptance testing
- 3) Engine/controller testing
- 4) Laboratory system testing.

### **Controller Qualification Testing**

Since the controllers are mounted directly on the Shuttle main engines, they are required to operate in a very severe environment during a mission. To assure that the unit can survive and operate correctly under such demanding conditions, an extensive design verification or qualification test program was developed and conducted. Portions of the qualification test program discussed are:

- 1) Acoustic vibration
- 2) Vibration
- 3) Thermal-vacuum
- 4) Operations
- 5) Interface fault testing
- 6) Electromagnetic interference.

The purpose of the acoustic vibration test was to evaluate the capability of the controller to function when subjected to the predicted Shuttle firing acoustic environments. The test controller was mounted in an acoustic test chamber by means of a soft suspension system and instrumented so that acceleration and acoustic data could be recorded. While powered up and operating in a mode that would detect functional failures, the controller was tested to a pre-defined acoustic noise spectrum with an overall sound pressure level of 153 dB over a frequency range of 10 to 10,000 Hz for a duration of 35 min.

The purpose of the vibration test was to verify the structural integrity, wear resistance, and operability of the controller when subjected to a simulated engine firing vibration environment. Three separate qualification vibration tests were run. The first vibration test program simulated the vibration induced during acceptance testing and was accomplished with the unit hardmounted (without rubber isolators) to the vibration fixture. Thirty minutes of random vibration, over the frequency spectrum of 20 to 2000 Hz, were run in each of the three axes. The overall composite reference level for each axis was approximately 11 Grms. The next vibration test program simulated the vibration induced during a 55 mission lifespan and consisted of 7.5 hr of random vibration in each axis. For this exposure, however, the controller was mounted to the fixture with the same type rubber isolators that are

used in the actual launch configuration. The spectrum used for this softmount vibration was also from 20 to 2000 Hz with a random composite reference level of approximately 22 Grms. The third vibration qualification test simulated engine-induced loads due to engine start and shutdown transients. To verify that the controller can survive such load forces applied during these times, 120 decaying sine pulses were applied in each of the three axes. The frequency and amplitude of the pulses applied were different for each axis, with the frequency being a function of the resonant frequency of that particular axis.

Throughout the entire vibration activity, the controller was operating in a mode that would detect any functional failures.

Qualification thermal-vacuum tests which consisted of approximately 60 cycles were performed on the controller design to verify that it could withstand the high and low temperatures associated with static firings, launch, on orbit storage and reentry/landing phases. The first portion of the thermal cycling tests consisted of 45 cycles with the controller in an operational state throughout. Each cycle consisted of test chamber effective temperature extremes of +125°F and -50°F and a cycle period of approximately 5 hr. A 2 hr dwell at high temperature and at low temperature plus transition times account for the 5 hr cycle. Command sequences were sent to the controller during the dwell times at both temperature limits to verify that all functional elements were operating without failures. During the next 10 cycles the temperature chamber was cycled between +125°F and -3°F. After a 2 hr dwell at low temperature, both computer channels were powered up and allowed to cycle so that any functional problems or failure to start cycling could be recognized. For the next five cycles, the chamber pressure was decreased below 1 mm of mercury at which time the controller was powered off. The chamber temperature was then cycled between +200°F and -80°F with only the controller heater voltage applied. Correct operation of the heater control element was confirmed by monitoring the temperatures at which the heater turned on and off.

An operations test was conducted on the SSME controller to verify that its design is capable of:

- 1) Accepting all specified sensor input signals and providing output commands for a specified engine power level.
- 2) Providing communication to and from the vehicle.
- 3) Monitoring and identifying failures.
- 4) Operating with a specified computer program.

Various means were used to satisfy the test objectives. These included the controller successfully supporting and controlling engine firings during the early engine development program. Correct signal and command interfacing was confirmed for each test firing by the normal data evaluation process. The remaining test objectives were achieved by certain functions being performed during acceptance testing on numerous controllers. All test results confirmed that the controller operated per requirements.

The objective of the interface fault insertion test was to verify that the controller is capable of safely withstanding faults at the controller/engine interface. For selected wires of each functional interface type, three different faults were inserted while the response of the controller to the faults was monitored and recorded. The types of faults injected into the system were:

- 1) Open selected inputs/outputs.
- 2) Short selected inputs/outputs to ground.
- 3) Short selected inputs/outputs to the highest voltage existing within its cable.

Electromagnetic Interference (EMI) testing was accomplished in two segments. The first was conducted at the controller component level in a laboratory environment, while the second was performed on an engine static test stand with a controller mounted on an engine. For the laboratory environment test, the controller was connected to an engine simulator. System level testing was then performed to verify that the controller is not susceptible to conducted EMI and does not generate conducted emissions in excess of the requirements. These tests were performed in an interference-free shielded enclosure within the laboratory. Successful completion of the emission tests verified that the controller, during flight readiness and flight operations, does not generate above-limit conducted emissions on the controller power interface nor radiate energy above the allowable limits. All major elements of the controller were exercised repeatedly throughout the test. The purpose of the susceptibility test was to verify that the controller's capability to accept and respond to vehicle commands is not degraded by specified EMI signal levels on the controller power interface, nor by specified level emissions from other nearby equipment.

The second segment of EMI testing performed on the controller was accomplished at the engine level. The controller was mounted on an engine in an actual static firing test stand. Although no controlled environment existed, an attempt was made to reduce external radiation by enclosing the sides of the test area with aluminum foil. The floor and ceiling around the engine were steel grating. Measurements confirmed that the aluminum foil reduced the external field by 10 dB. Conducted and radiated tests were then performed while the controller operated in several different modes. Again it was confirmed that the controller does not generate above-limit conducted emissions, nor radiate above acceptable levels. Acceptable controller operation was also demonstrated with susceptibility testing.

No controller hardware design changes were made due to the EMI test program, and no concerns were identified which suggested the controller would not operate as required.

### **Acceptance Testing**

A great deal of testing is performed at various subassembly and screening levels before each controller is ready for final functional acceptance testing. Testing actually starts at the piece part level prior to populating the printed circuit cards. After they have been populated, the cards are then subjected to tests which verify that they have been built

correctly and that they function properly. These cards are tested at different temperature levels by a computer-controlled automatic test station which applies stimuli to the card and monitors for correct response on the appropriate control or signal lines. Passing these tests assures that the functions of the card will perform error free at the next higher assembly level. Some circuit cards are then integrated into subassemblies, such as power supplies and memory systems, and tested at this intermediate level prior to installation into the controller chassis.

After the controller chassis has been fully loaded with printed circuit cards and subassemblies, it is subjected to debug tests. Debug testing confirms that all cable interconnections within the controller have been mated properly and that there are no open or short circuits within the controller which may have been created by the final assembly. After successful completion of the debug tests, the controller is ready to begin formal acceptance tests.

The acceptance test flow consists of both operational testing and mechanical operations. The main areas of operational tests are the functional, thermal cycle, and vibration. Functional tests are performed with the controller connected to a sophisticated and critical piece of computer based test equipment which simulates an Orbiter main engine. Special test software is loaded into channel A and channel B controller memory at the start of formal acceptance testing and is used throughout the test cycle. As can be seen in Figure 14 the interface of the controller to the test equipment is very extensive and consists of over a thousand control, power, test, signal, and ground wires. The controller test results are monitored by the automatic test equipment which reports any anomolous or failure conditions.

Thermal cycle testing of the controller consists of eight cycles, each one approximately 5 hr in duration. During each cycle, the controller is exposed to a temperature of +125°F and -50°F for a minimum of 2 hr each. The controller is powered up and cycling in the acceptance test software throughout the eight cycles, so that any failures which occur can be recognized and reported.

For the vibration portion of acceptance testing, the controller is hard-mounted to the vibration test fixture. That is, the elastomeric shock isolators are not used. The controller is then vibrated at a level of approximately 7 Grms random in the three mutually orthogonal axes for a period of 10 min each. During vibration, the controller is connected to a simulated engine and operated in a self-test mode which includes monitoring all input and output signals. Any failures which occur are recognized and reported.

Among the mechanical operations performed during acceptance testing are: a controller proof pressure test at a pressure of 44.2 psig; final pressurization of the controller to a 23.5 psia value using nitrogen and helium; and verifying that the leak rate of the controller chassis is less than  $2.9 \times 10^{-4}$  standard cubic centimeters of helium per second at one atmosphere differential.

After successful completion of the above acceptance test flow, the controller is ready to be mounted on an engine.

## Engine/Controller Tests

All engine development hot-fire tests are performed using controllers. During the early phases of the development program, a rack-mounted controller was remotely located from the engine and used for engine monitor and control. As the engine development progressed and as prototype controllers became available, the controllers were mounted directly on the engines to support hot-firing tests. This configuration afforded a method of testing controller hardware, flight software, and engine development in parallel. Later in the program a three engine cluster was assembled and test fired numerous times to simulate, as much as possible, an orbiter launch configuration. At the time of the first Shuttle launch, controllers had supported over 630 single engine firings, and 17 cluster firings for an accumulated engine firing time of over 100,000 sec.

## Laboratory System Testing

To facilitate flight software development, a hardware simulation laboratory was built at the NASA/MSFC. The hardware was configured to simulate, as closely as possible, the interfaces a controller interacts with to monitor and control engine operation. As the controller hardware matured into the final flight configuration, a controller of the latest design available was furnished to the simulation laboratory to be used for software development. In this manner, one of the original design goals of developing hardware and software in parallel was accomplished. Any controller/system or software problems found during these system level tests were quickly recognized, reported, and corrected.

## OPERATIONAL FUNCTIONS AND TIMELINES

The approach to developing flight software for the controller was to create one main program, called the executive program, and several special purpose subprograms. The executive program has the primary task of supervising the sequence of processing subprograms when needed and keeping track of the total status of the engine, avionics, and commands from the vehicle. Operation of the executive program is cyclic with a complete cycle (major cycle) through the executive program being completed every 20 msec. Under normal operation, whether on the ground during prelaunch checkout, or during flight, the computer progresses through the executive program, performing the required operations in an endless loop. The loop is broken and the sequence of operations is revised by any of several possible events:

- 1) A command is received from the Orbiter which alters the control or checkout phase of operation.
- 2) Built-in testing determines that a failure has occurred.
- 3) Engine-monitoring detects a parameter which has exceeded allowable limits.

Figure 14 is a simplified flow chart of the executive program. The major cycles are divided into four 5 msec processing intervals called minor cycles. Each minor cycle has associated with it certain tasks that are to be performed. These tasks may be performed only within that one minor cycle of the major cycle, or may be performed in multiple minor cycles within the major cycle. Major overall tasks that the software executes are:

- 1) Process inputs from pressure, temperature, position, shaft speed, and flowrate sensors.
- 2) Control the operation of servovalves, actuators, solenoids, servoswitches, and spark igniters.
- 3) Accept and process commands from the Orbiter.
- 4) Provide and transmit data to the Orbiter.
- 5) Provide checkout and monitoring capabilities to ensure controller fail-operational, fail-safe capability.

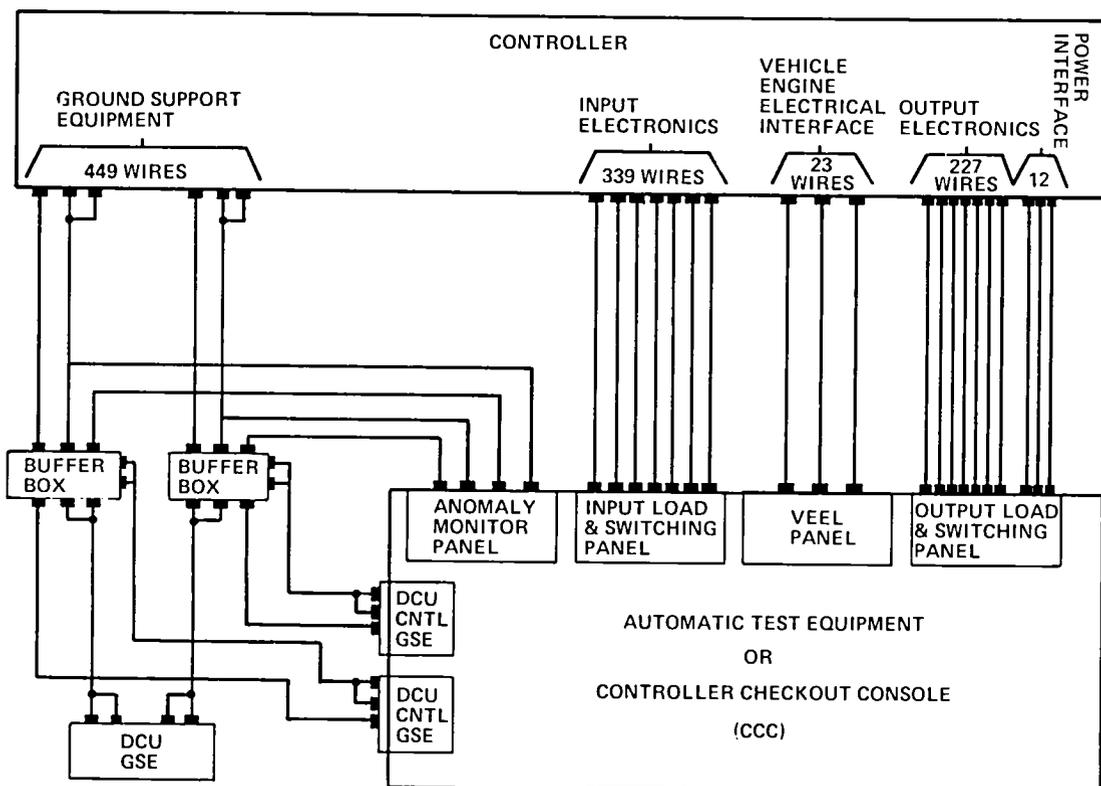


Figure 14. System test configuration.

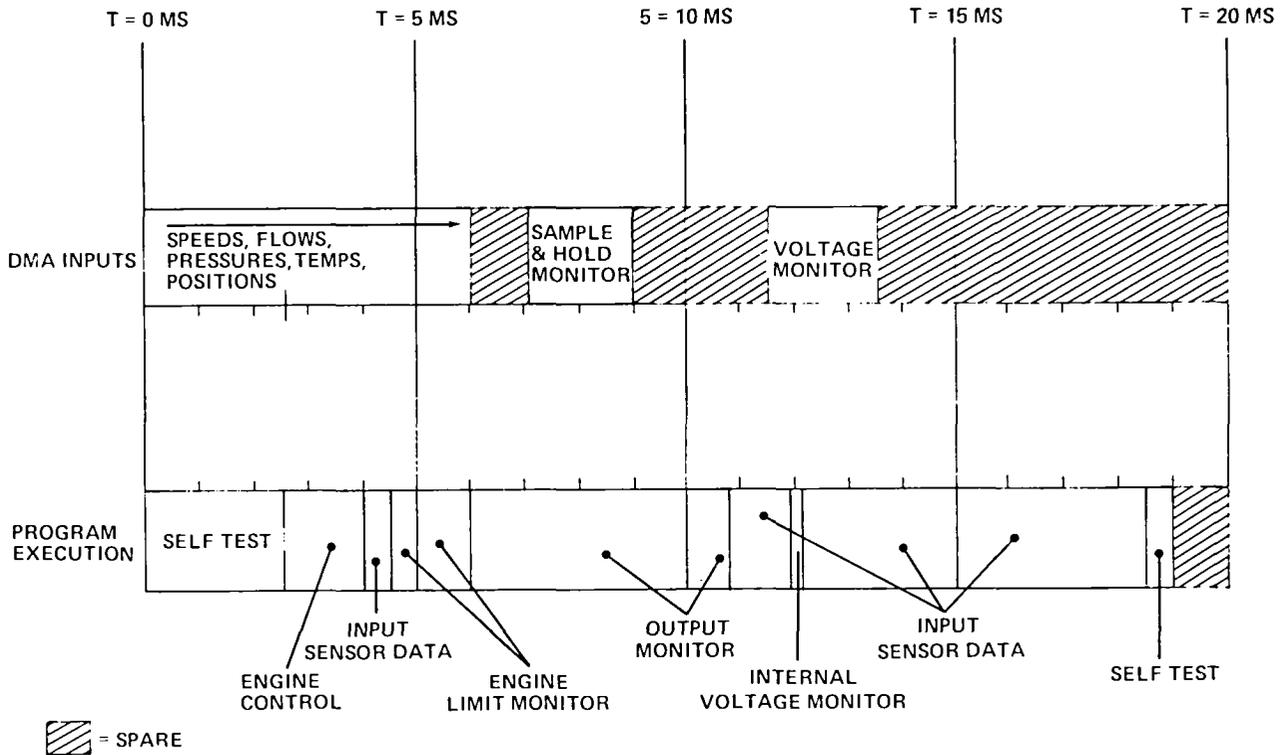


Figure 15. Major cycle timing.

## OPERATIONAL EXPERIENCE

The controller build and delivery activity can be identified as consisting of three periods: A, B, and C. The first two controllers delivered in period A were rack-mounted designs which were used to verify the functional capability of the design and to support early engine firings. Also in period A, four prototype controllers were built with the same packaging concept and overall envelope as the final design and were used for laboratory testing and engine firings. At the time of the first Shuttle flight, the period A controllers had accumulated a total field and laboratory run time of over 40,000 hr. In period B, 12 units of the final flight design package were built and delivered. Controllers delivered in this period were used for qualification testing, single engine development firings, engine cluster firings, software development, and the first Shuttle launch. As of the first Shuttle launch, the period B controllers had accumulated a total run time of over 42,000 hr. Fifteen controllers are scheduled to be delivered in the period C part of the program. All will be of the latest flight design and will be assigned to flight engines, flight spares, or advanced engine test support as they are built.

## CONCLUSIONS

The vast amount of engine hot-fire time that the controllers have successfully supported demonstrates that the original concept of a digital control system for the SSME as well as the hardware/software implementation of that system is sound. Successful completion of the first Shuttle Columbia launch in April 1981 further confirms that the controller can withstand the harsh environment encountered during a flight and at the same time fulfill the operational and functional requirements for which it was designed.

## BIBLIOGRAPHY

Controller and Software Reference Handbook. RSS-8628, December 15, 1978.

Failure Mode and Effects Analysis, P6 Flight 2. Vol. IV and Vol. XII, W2107-FMEA-P6/  
Flt 2B, November 1, 1979.

Mitchell, Walter T.: Space Shuttle Main Engine Digital Controller.

Engine Design Definition Report RSS-8502-2, DRD-SE-275, Computer Program Contract  
End Item DS25648-01, Honeywell.

DVS Test Reports: Vibration, RSS-201-109; Thermal Cycle, RSS-201-108; EMI, RSS-201-  
110 and RSS-101-58; Controller Operations, RSS-201-112; and Acoustic Vibration,  
RSS-201-96.

|  |  |   |                                 |
|--|--|---|---------------------------------|
| 1. REPORT NO.<br>NASA TP-1932  | 2. GOVERNMENT ACCESSION NO.                              | 3. RECIPIENT'S CATALOG NO.  |                                 |
| 4. TITLE AND SUBTITLE<br><br>Space Shuttle Main Engine Controller  |  | 5. REPORT DATE<br>November 1981   | 6. PERFORMING ORGANIZATION CODE |
|  |  | 8. PERFORMING ORGANIZATION REPORT #   |                                 |
| 7. AUTHOR(S)<br>Russell M. Mattox and J. B. White  |  | 10. WORK UNIT NO.<br>M-360  |                                 |
| 9. PERFORMING ORGANIZATION NAME AND ADDRESS<br><br>George C. Marshall Space Flight Center<br>Marshall Space Flight Center, Alabama 35812   |  | 11. CONTRACT OR GRANT NO.   |                                 |
|  |  | 13. TYPE OF REPORT & PERIOD COVERED<br><br>Technical Paper                                |                                 |
| 12. SPONSORING AGENCY NAME AND ADDRESS<br><br>National Aeronautics and Space Administration<br>Washington, D.C. 20546  |  | 14. SPONSORING AGENCY CODE  |                                 |
| 15. SUPPLEMENTARY NOTES<br><br>Prepared by Data Systems Laboratory, Flight Computer Branch   |  |   |                                 |
| 16. ABSTRACT<br><br><p>A technical description of the Space Shuttle Main Engine Controller, which provides engine checkout prior to launch, engine control and monitoring during launch, and engine safing and monitoring in orbit, is presented. Each of the major controller subassemblies, the central processing unit, the computer interface electronics, the input electronics, the output electronics, and the power supplies are described and discussed in detail along with engine and orbiter interfaces and operational requirements.</p> <p>The controller represents a unique application of digital concepts, techniques, and technology in monitoring, managing, and controlling a high performance rocket engine propulsion system. The operational requirements placed on the controller, the extremely harsh operating environment to which it is exposed, and the reliability demanded, result in the most complex and ruggedized digital system ever designed, fabricated, and flown.</p> |  |   |                                 |
| 17. KEY WORDS<br><br>Shuttle Main Engine Control Electronics<br>Control Electronics (Computer)   |  | 18. DISTRIBUTION STATEMENT<br><br>Unclassified - Unlimited<br><br><br>Subject Category 60 |                                 |
| 19. SECURITY CLASSIF. (of this report)<br><br>Unclassified   | 20. SECURITY CLASSIF. (of this page)<br><br>Unclassified | 21. NO. OF PAGES<br><br>39  | 22. PRICE<br><br>A03            |



National Aeronautics and  
Space Administration

Washington, D.C.  
20546

Official Business

Penalty for Private Use, \$300

THIRD-CLASS BULK RATE

Postage and Fees Paid  
National Aeronautics and  
Space Administration  
NASA-451



**NASA**

POSTMASTER: If Undeliverable (Section 158  
Postal Manual) Do Not Return

---